UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/840,492	04/23/2001	Thomas A. Liebert	2000-2088	5712

7590   10/22/2004

Samuel H. Dworetsky
AT&T CORP.
P.O. Box 4110
Middletown, NJ 07748-4110

EXAMINER
LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

> A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
> - Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
> - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
> - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
> - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>23 April 2001</u>.

2a)☐ This action is **FINAL**.　　2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-11</u> is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-11</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☐ All　b)☐ Some * c)☐ None of:

　　　1.☐ Certified copies of the priority documents have been received.

　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>2</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims **1-11** have been examined.

Specification

2.   The disclosure is objected because of the following informalities:

*   On page 1, the last line "a cable modem or "CM", has been mentioned with

respect to figure 1, nevertheless the disclosure did not indicate or give a reference to indicate

the location of the Cable Modem or "CM" on figure 1.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form

the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4.   **Claim 1** is rejected under 35 U.S.C. 102(e) as being anticipated by Kalmanek, Jr. et al.

(hereinafter referred to as Kalmanek) (U.S. Patent No. 6,483,912).

5.   **As per claim 1**, Kalmanek discloses a method of Quality of Service Signaling in a

system for cable telephony using one or more packet data networks, comprising the steps of:

•   Encrypting, at an Internet Protocol Digital Terminal, a Dynamic

Quality of Service signaling message; and (Column 6, lines 17-26) (As explained on

submitted disclosure on page 2, ref. Num [0005], lines 12-15, "an Internet Protocol

Digital Terminal" is a device that is connected to the IP network to send signals to

and receive signals from a "CMTS/ER". The office interpreted the "Gate Controller"

which is shown on figure 1 as an Internet Protocol Digital Terminal" since it is a

device that is connected to IP network which is shown on figure 1, ref. Num "100"

and send signals to and receive signal from a "CMTS/ER". The "Network edge

device" which is shown on figure 1, ref. Num "120" and "121", performs the task of

"CMTS/ER" as explained on column 5, lines 7-26. Accordingly, as explained on

column 6, lines 17-26, the dynamic quality of service signaling message which

includes different information. Such information is explained to be encrypted and

sent to the "TIUS" which is also called BTIs as explained on column 5, lines 41-44,

from the "Gate controller" as explained on column 6, lines 17-26 and this meets the

recitation of this limitation)

•   Transmitting; a signaling message including said encrypted Dynamic

Quality of Service signaling message to a Broadband Telephony Interface. (Column

6, lines 17-26)

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.   **Claim 2** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chapman.

(hereinafter referred to as Chapman) (U.S. Patent No. 6,182,104) in view of Kalmanek, Jr. et al.

(hereinafter referred as Kalmanek)(U.S. Patent No. 6,483,912)

8.   **As per claim 2, Chapman** discloses a method of Quality of Service Signaling in a

system for cable telephony using one or more packet data networks, comprising the steps

of

•   Receiving, at a Cable Modem Termination System, a signaling

message including an encrypted Dynamic Quality of Service signaling message from a

Broadband Telephony Interface or "CM" or cable modem in connection with a request to

change access by said Broadband Telephony Interface to network resources; (column 9,

lines 7-23; column 2, lines 41-46; column 4, lines 45-52).(the request to change access by

"CM" cable modem to network resources meets the recitation of this limitation and the

packet that includes the quality of service message is encrypted as explained on column 4,

lines 45-50.)

Furthermore, **Chapman** further discloses controlling, access by said Broadband Telephony Interface or "CM" or cable modem to network resources in accordance with the, results of or the decision made by CTMS by checking the authorization of the request which comes from the Broadband Telephony Interface or "CM" or cable modem (Column 9, lines 15-22)

Chapman does not explicitly teach

- Attempting to decrypt said encrypted Dynamic Quality of Service signaling message; and controlling, access by said Broadband Telephony Interface to network resources in accordance with the, results of said decryption attempting step. However, **Kalmanek,** in the same art of endeavor discloses that BTIs or Broadband Telephony Interface sends a trace message containing its own authentication information to the gate controller and the gate controller verifies the connection information or request by decrypting and checking the signature. (column 53, lines 55-62)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to add the features of decryption and checking the authorization request of the Broadband Telephony Interface to control the access as per teachings of Kalmanek into the controlling change access request verification method as taught by Chapman in order to decrypt and verify the encrypted authorization request before granting control change access to the Broadband Telephony Interface.

9.   **Claims 3-5 and 9-11** are rejected under 35 U.S.C. 103(a) as being unpatentable kalmanek, Jr. et al. (hereinafter referred as Kalmanek)(U.S. Patent No. 6,483,912) in view of Chapman. (hereinafter referred to as Chapman) (U.S. Patent No. 6,182,104)

10.   **As per claim 3 and 9, Kalmanek** discloses a method of Quality of Service Signaling in

a system for cable telephony using one or more packet data networks, comprising the steps of

- Encrypting at an Internet Protocol Digital Terminal, a Dynamic

Quality of Service signaling message using an encryption key; (Column 6, lines 17-

26) (As explained on submitted disclosure on page 2, ref. Num [0005], lines 12-15,

"an Internet Protocol Digital Terminal" is a device that is connected to the IP

network to send signals to and receive signals from a "CMTS/ER". The office

interpreted the "Gate Controller" which is shown on figure 1 as an Internet Protocol

Digital Terminal" since it is a device that is connected to IP network which is shown

on figure 1, ref. Num "100" and send signals to and receive signal from a

"CMTS/ER". The "Network edge device" which is shown on figure 1, ref. Num "120"

and "121", performs the task of "CMTS/ER" as explained on column 5, lines 7-26.

Accordingly, as explained on column 6, lines 17-26, the dynamic quality of service

signaling message which includes different information. Such information is

explained to be encrypted and sent to the "TIUS" which is also called BTIs as

explained on column 5, lines 41-44, from the "Gate controller" as explained on

column 6, lines 17-26 and this meets the recitation of this limitation) and

- Transmitting a signaling message including said encrypted Dynamic

Quality of Service signaling message from said Internet Protocol Digital Terminal to

a Broadband Telephony Interface; (Column 6, lines 17-26)

Furthermore

- **Kalmanek,** discloses that BTIs or Broadband Telephony Interface

sends a trace message containing its own authentication information to the gate

controller and the gate controller verifies the connection information or request by

decrypting and checking the signature. (column 53, lines 55-62)

Kalmanek does not explicitly teach

- Transmitting a signaling message including said encrypted Dynamic Quality of Service signaling message from said Broadband Telephony Interface to a Cable Modem Termination System in connection with a request to change access by said Broadband Telephony Interface to network resources;

- Controlling access by said Broadband Telephony Interface to network resources in accordance with the results of said decryption attempting step. However, **Chapman,** in the same art of endeavor discloses

- Receiving, at a Cable Modem Termination System, a signaling message including an encrypted Dynamic Quality of Service signaling message from a Broadband Telephony Interface or "CM" or cable modem in connection with a request to change access by said Broadband Telephony Interface to network resources; (column 9, lines 7-23; column 2, lines 41-46; column 4, lines 45-52).(the request to change access by "CM" cable modem to network resources meets the recitation of this limitation and the packet that includes the quality of service message is encrypted as explained on column 4, lines 45-50.)

- Furthermore, **Chapman** further discloses controlling, access by said Broadband Telephony Interface or "CM" or cable modem to network resources in accordance with the, results of or the decision made by CTMS by checking the authorization of the request which comes from the Broadband Telephony Interface or "CM" or cable modem (Column 9, lines 15-22)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to add the features of controlling change access request verification method as per teachings of Chapman into the encryption and decryption

method for checking the authorization request of the Broadband Telephony Interface as

taught by Kalmanek in order to request change access by Broadband Telephony

Interface to the network resources.

11.   **As per claim 4 and 10,** the combination of Kalmanek and Chapman discloses the

the method as applied to claims 3 and 9 above. Furthermore, Kalmanek discloses the

method wherein said encrypted Dynamic Quality of Service signaling message transmitted

in step (b) is part of a Create Connection (CRCX) or Delete Connection (DLCX) message.

(column 32, lines 47-50)

12.   **As per claim 5 and 11**, the combination of Kalmanek and Chapman discloses the

the method as applied to claims 3 and 9 above. Furthermore, Chapman discloses the

method wherein said encrypted Dynamic Quality of Service signaling message transmitted

in step (c) is part of a Dynamic Service Addition Request (DSA-REQ) or Dynamic Service

Delete Request (DSD-REQ) message. (Column 5, lines 50-61)

13.   **Claims 6-8** are rejected under 35 U.S.C. 103(a) as being unpatentable kalmanek, Jr. et

al. (hereinafter referred as Kalmanek)(U.S. Patent No. 6,483,912) in view of Chapman.

(hereinafter referred to as Chapman) (U.S. Patent No. 6,182,104) further in view of Heer et al

(hereinafter referred as Heer) (U.S. Patent No. 6,028,933)

14.   **As per claim 6,** the combination Kalmanek and Chapman discloses the method as

        applied to claims 3 above. Furthermore, Kalmanek discloses

        Encrypting, at an Internet Protocol Digital Terminal, a Dynamic Quality of Service

        signaling message; and (Column 6, lines 17-26) (As explained on submitted

disclosure on page 2, ref. Num [0005], lines 12-15, "an Internet Protocol Digital

Terminal" is a device that is connected to the IP network to send signals to and

receive signals from a "CMTS/ER". The office interpreted the "Gate Controller"

which is shown on figure 1 as an Internet Protocol Digital Terminal" since it is a

device that is connected to IP network which is shown on figure 1, ref. Num "100"

and send signals to and receive signal from a "CMTS/ER". The "Network edge

device" which is shown on figure 1, ref. Num "120" and "121", performs the task of

"CMTS/ER" as explained on column 5, lines 7-26. Accordingly, as explained on

column 6, lines 17-26, the dynamic quality of service signaling message which

includes different information. Such information is explained to be encrypted and

sent to the "TIUS" which is also called BTIs as explained on column 5, lines 41-44,

from the "Gate controller" as explained on column 6, lines 17-26 and this meets the

recitation of this limitation)

The combination of Kalmanek and Chapman does not explicitly teach encryption

key is a private encryption key and said decryption key is a public encryption key

for use in a system of public key cryptography.

However in the same art of endeavor **Heer** discloses implementing creation and

verification algorithms with unidirectional and asymmetric public key

algorithm.(column 3, lines 41-44)

It would have been obvious to one having ordinary skill in the art, at the time the

invention was made, to combine the use of public key cryptography as per teachings of

Heer into the encryption and decryption method taught by the combination of

Kalmanek and Chapman in order to secure the communication.

15.   **As per claim 7 and 8,** the combination Kalmanek and Chapman discloses the method

as applied to claims 3 above. Furthermore, Kalmanek discloses

Encrypting, at an Internet Protocol Digital Terminal, a Dynamic Quality of Service

signaling message; and (Column 6, lines 17-26) (As explained on submitted

disclosure on page 2, ref. Num [0005], lines 12-15, "an Internet Protocol Digital

Terminal" is a device that is connected to the IP network to send signals to and

receive signals from a "CMTS/ER". The office interpreted the "Gate Controller"

which is shown on figure 1 as an Internet Protocol Digital Terminal" since it is a

device that is connected to IP network which is shown on figure 1, ref. Num "100"

and send signals to and receive signal from a "CMTS/ER". The "Network edge

device" which is shown on figure 1, ref. Num "120" and "121", performs the task of

"CMTS/ER" as explained on column 5, lines 7-26. Accordingly, as explained on

column 6, lines 17-26, the dynamic quality of service signaling message which

includes different information. Such information is explained to be encrypted and

sent to the "TIUS" which is also called BTIs as explained on column 5, lines 41-44,

from the "Gate controller" as explained on column 6, lines 17-26 and this meets the

recitation of this limitation)

The combination of Kalmanek and Chapman does not explicitly teach the step of

distributing and generating said keys.

However in the same art of endeavor **Heer** discloses steps of distributing keys

(Column 27, lines 29-49) and generating keys (Column 26, lines 31-47)

It would have been obvious to one having ordinary skill in the art, at the time the

invention was made, to combine the steps of generating and distributing keys as per

teachings of Heer into the encryption and decryption method taught by the combination

of Kalmanek and Chapman in order to create and distribute a key.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4:30 pm).
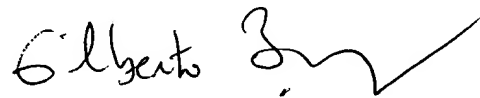
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

10/18/2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100